

Chetham's

Data Protection Policy

5/11/26

Owner: JAR-C
Line Manager: NS
Created: JAR-C 12/10/21
Version: 5/11/26
Review: 5/11/27

Chetham's

Data Protection Policy

1. Aims

Chetham's aims to ensure that all personal data collected about staff, students, parents, carers, guardians, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR); the Data Protection Act 2018 (DPA 2018); UK Data (Use and Access) Act 2025 (UDUA); and non-statutory guidance from the DfE Generative Artificial Intelligence in Education 8.25, as well as Part 7 of the *Independent Schools Regulations Guidance* 2026.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation And Guidance

This policy meets the requirements of the GDPR; UDUA; and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Please note that Chetham's is not a public body and is, therefore, not subject to the Freedom of Information Act 2000.

3. Definitions

PHRASE	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

PHRASE	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health; physical or mental • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and pays its data protection fee to the ICO annually, as legally required.

5. Roles And Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

He will provide an annual report of his activities directly to the Governing Body and, where relevant, report to the board his advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Jon Runswick-Cole who is contactable via dpo@chethams.com / 01618387200 extn 123.

Joint Principals
The Joint Principals act as the representatives of the data controller on a day-to-day basis.

All Staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties.

6. Data Protection Principles

The GDPR is based on data protection principles with which our school must comply.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- Any automated processing or use of generative AI will be monitored and finally decided by a human.

This policy sets out how the School aims to comply with these principles.

7. Collecting Personal Data

Lawfulness, Fairness And Transparency
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract
2. The data needs to be processed so that the School can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
4. The data needs to be processed so that the School, as a public authority, can **perform a task in the public interest or exercise its official authority**
5. The data needs to be processed for the **legitimate interests** of the School (where the processing is not for any tasks the School performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
6. The individual (or their parent/carer/guardian when appropriate in the case of a student) has freely given clear **consent**
7. For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:
8. The individual (or their parent/carer/guardian when appropriate in the case of a student) has given **explicit consent**
9. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
10. The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
11. The data has already been made **manifestly public** by the individual
12. The data needs to be processed for the establishment, exercise or defence of **legal claims**
13. The data needs to be processed for reasons of **substantial public interest** as defined in legislation
14. The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
15. The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
16. The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest
17. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:
    - The individual (or their parent/carer/guardian/guardian when appropriate in the case of a student) has given **consent**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

18. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
19. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, Minimisation And Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in accordance with the School's record retention schedule.

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- there is an issue with a student or parent/carer/guardian that puts the safety of our staff at risk
- we need to liaise with other agencies; we will seek consent as necessary before doing this
- our suppliers or contractors need data to enable us to provide services to our staff and students; for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law including the Age Appropriate Design Code.
    - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so including crime prevention.

We may also share personal data with emergency services, public bodies and local authorities to help them to respond to an emergency that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject Access Requests And Other Rights Of Individuals

Subject Access Requests
Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:

1. Confirmation that their personal data is being processed
2. Access to a copy of the data
3. The purposes of the data processing
4. The categories of personal data concerned
5. Who the data has been, or will be, shared with
6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
7. Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
8. The right to complain following the School's Concerns and Complaints Policy and if not resolved then complain to the ICO (https://ico.org.uk) or alternative authority
9. The source of the data, if not the individual
10. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
11. The safeguards provided if the data is being transferred internationally
12. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
    - Name of individual
    - Correspondence address
    - Contact number and email address
    - Details of the information requested
    - If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children And Subject Access Requests
Personal data about a child belongs to that child, and not the child's parents guardians or carers. For a parent, guardian or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

In Scotland a person aged 12 or above is considered to have the maturity to exercise their right of access. However, in England competence is assessed depending on the child's level of understanding of their rights and the implications of a subject access request. A student's ability to understand their rights will always be judged on a case-by-case basis. A child's competence may change over time. Generally a child is not considered competent to make a SAR if they are acting against their own best interests.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students over the age of 12 at our school may not be granted without the express permission of the student. This is not a rule and a

student's ability to understand their rights will always be judged on a case-by-case basis.

Responding To Subject Access Requests (SARs)
When responding to requests, we:

1. May ask the individual to provide 2 forms of identification and full contact details
2. May contact the individual via phone to confirm their identity and the request scope
3. Will respond without delay and within 1 month of receipt of the request and after clarification of the data required and receipt of the additional information needed to confirm identity, where relevant
4. Will provide the information free of charge
5. May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or has numerous strands. We will inform the individual of this within 1 month, and explain why the extension is necessary
6. SARs must be reasonable and proportionate. The clock is stopped whilst we discuss the precise terms of the SAR. We will only process reasonable and proportionate requests.

We may not disclose information for a variety of reasons, such as if it:

1. might cause serious harm to the physical or mental health of the student or another individual
2. would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
3. would include another person's personal data that we can't reasonably anonymise, and/or we don't have the other person's consent and/or it would be unreasonable to proceed without their permission
4. is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
5. is an unfounded, or excessive request, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive or vexatious when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to follow our complaints procedure and thereafter complain to the ICO or they can seek to enforce their subject access right through the courts.

Other Data Protection Rights Of The Individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

1. Withdraw their consent to processing at any time
2. Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
3. Prevent use of their personal data for direct marketing
4. Object to processing which has been justified on the basis of public interest, official authority or legitimate interests

5. Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
6. Be notified of a data breach (in certain circumstances)
7. Make a complaint to the School: see the School's Concerns and Complaints Policy
8. Make a complaint to the ICO, after completing the School's Complaints Procedures
9. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
10. Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO: dpo@chethams.com

10. Parental Requests To See The Educational Record

The Education (Pupil Information) (England) Regulations 2005 do not apply to Chetham's as we are a non-maintained school.

However, the Education (Independent School Standards) Regulations 2026, set out minimum standards for independent schools like ours. The standards on information provision require that we provide an annual written report of each registered pupil's progress and attainment in the main subject areas taught to the parents of that registered pupil. Parents are entitled to see tutor cards and profiles which constitute our reporting system.

There are certain circumstances in which this right can be denied, for example: if releasing the information might cause serious harm to the physical or mental health of the student or another individual; or if it would mean releasing exam marks before they are officially announced.

Students have right of access under article 15 of the UK GDPR. Parents can only submit a SAR for information about their child if the child is not competent to act on their own behalf or has given their consent. However, we will need evidence that the student has authorised the parent to make the SAR.

11. Biometric Recognition Systems

We do not currently use any biometirec recognition systems.

12. Generative Artificial Intelligence

We do use a few Artificial Intelligence products, such as CoPilot, to process data and we are aware of our responsibilities:

Any such AI products have to meet the following minimum criteria before we use them:

- Prevent access to harmful and inappropriate content
- Robust activity logging procedures
- Secure against malicious use or exposure to harm
- Robust data handling and transparency around processing of personal data
- Does not collect or store intellectual property created by students or copyright owner for commercial purposes
- Transparent systems which safeguard children by design
- Accountability and human oversight
- Ongoing Risk Monitoring

- Meet our Safeguarding and legal duties

13. CCTV

We use CCTV in various locations around the School site to ensure everyone remains safe. We adhere to the Home Office Surveillance Camera Code of Practice 2021 for the use of CCTV. It is never used to intrude.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Only SIA CCTV Operator License trained Security staff are able to access our securely encrypted CCTV footage, which usually has a 30-day erase cycle. The CCTV room has a member of staff assigned 24/7.

Other than viewing by the Security staff for routine surveillance purposes, additional, CCTV footage may not be viewed or shared without prior approval from a member of the SLT, usually the DPO or the Facilities and Site Manager, for specific purposes such as, but not limited to: confirming a sequence of events; safeguarding; prevention and detection of crime; fulfilling a legal obligation; public safety; protection of rights; national security.

Any enquiries about the CCTV system should be directed to the Facilities and Site Manager, who has overall responsibility, but delegates to the DPO on matters of data sharing and viewing.

14. Photographs And Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers/guardians for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used, to the parent/carer/guardian and student.

Any photographs and videos taken by parents/carers/guardians at School events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

We will obtain written consent from parents/carers/guardians, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer/guardian and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers/guardians at School events for their own personal use, such as family album or to share with close friends, are not covered by data protection legislation. However, such images which include other students, must not be shared publicly on social media or by any other means, nor manipulated using AI, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Photos and videos taken by parents must not disrupt the event; or cause safeguarding concerns.

Staff, volunteers, visitors and contractors are not permitted to take photos or videos for their personal or public use on personal devices.

Where the School takes photographs and videos, (*school origin image content*), they must be taken on school equipment and held in school storage devices / cloud. They must not be taken or stored on personal devices or cloud accounts. School uses may include:

- Within school on swipe cards, notice boards and in school magazines, brochures, newsletters, etc
- Outside of school by external agencies such as the School photographer, newspapers, campaigns
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

School origin image content must not be re-broadcast or digitally manipulated with or without AI by third parties including parents and students except with the express permission of the School.

We use low resolution or watermarked images on our website to deter AI manipulation of our digital media.

School held images will be subject to our usual record retention policy and procedures.

See our *Safeguarding and Child Protection Policy* and *Online Activity and Procedures Policy* for more information on our use of photographs and videos.

15. Data Protection By Design And Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

1. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
2. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
3. Completing data protection impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
4. Integrating data protection into internal documents including this policy, any related policies and privacy notices
5. Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
6. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
7. Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
8. Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our Privacy Notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

16. Data Security And Storage Of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

1. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
2. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
3. Where personal information needs to be taken off site, staff must sign it in and out from the School office
4. Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites
5. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
6. Personal information should only be stored on One Drive to reduce the risk of data breaches. Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our *AUP* and *Online Activity* policies).
7. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

17. Disposal Of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal Data Breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students.

19. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

20. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy at least annually and sharing with the full governing body.

21. If You Communicate With Us Through Social Media

If you choose to interact with our Website, or content through social media such as LinkedIn, Facebook; your personal data (such as your name and the fact that you are interested in Chets) will also be visible to all the visitors of your personal webpage on LinkedIn, Facebook etc, according to your privacy settings on the social media services. Chetham's is not responsible for the processing of personal data or the privacy policy of such social media websites. Chetham's no longer has an account with X.

22. Cookies And Similar Technologies

We may use cookies and similar technologies that aim to collect and store information when you visit a Chets website. The main purpose of cookies is to allow us to identify your internet browser and collect data on your use of our website, which pages you visit, the duration of your visits and identify these when you return. These technologies are also used in order to collect and store information about your interaction with our services. You may control, reject and set cookies by checking your browser settings.

23. Resources

Surveillance Camera Code of Practice

Independent School Standards Guidance 2026

ICO: Education Information

ICO: Requests for Info about children

ICO: Taking Photographs in schools

ICO: Complaints

ICO: Accessing Pupil's Info

Appendix 1:

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) at dpo@chethams.com.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people.

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Joint Principal (JS) and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's Sharepoint site.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the School's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the School's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where the School is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals; for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on the Chetham's Sharepoint site.

The DPO and Joint Principal (NS) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and Joint Principal (NS) will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the School to reduce risks of future breaches.

Actions To Minimise The Impact Of Data Breaches
Essentially the actions for any data breach are the same:

- Acknowledge the breach
- Act to recover / stem the flow of data
- Inform the DPO asap who will decide whether ICO need to be informed and
- Discuss options for mitigating the impact of the breach
- Inform relevant parties of the breach
- DPO records the breach
- DPO reviews procedures and actions with Joint Principal (NS) and makes recommendations to minimize the chance of subsequent breaches.

The steps outlined below show a typical response sequence.

Sensitive Information Disclosed Via Email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error and alert the DPO who will advise on next steps

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO / staff will ask IT support to attempt to recall it from external recipients and remove it from the School's email system, retaining a copy if required as evidence
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The staff / DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher / website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the staff / DPO will inform the DSL who will then follow our safeguarding procedures.